International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Research Paper on Android Graphical Image Password

Raja Saha, Dr. Umarani Chellapandy

Department of MCA, Jain Deemed-to-be-University, Bangalore, Karnataka, India

ABSTRACT

Security of authentication is needed to be provided superlatively to secure users 'personal and exchange information, since online information exchange systems, have been developed according to internet speed. Therefore, the aim of the chapter is to develop a current graphical password scheme based on recall and create and implement anew graphical password scheme composed of three-layer verification. We programmed our scheme in order to use in a section of anonymous information exchange system and user's registration of trading chat room. While we conducted survey on users by accessing participants to our system lied in participants' local network and we analyzed in accordance with the average length of their created password and statistical significance of entropy bit. From the survey of total participants, our scheme has statistical significance, furthermore, it was proved that it can secure from a variety of attacks as entropy bit was high.

KEYWORDS: *Smart Phones, Graphical Passwords, Authentication, Network Security*

How to cite this paper: Raja Saha | Dr. Umarani Chellapandy "Research Paper on Android Graphical Image Password" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.1903-1904, URL: www.ijtsrd.com/papers/ijtsrd49859.pdf

IJTSRD49859

INTRODUCTION

In a graphical password, a user interacts with one or more images to create or enter a password. Graphical passwords are intended to capitalize on the promise of better memorability and improved security against guessing attacks. Graphical passwords are particularly suitable for keyboard-less devices such as iPods and iPhones whereon inputting a text password is cumbersome. For example, Windows 8 recently released by Microsoft supports graphical password logon. With the increasing popularity of smartphones and slate computers, we expect to see the wider deployment of graphical passwords in Web applications. The project allows users to input an image as its password and only the user knows what the image looks like as a whole. On receiving the image, the system segments the image into an array of images and stores them accordingly. The next time user logs on to the system the segmented image is received by the system in a jumbled order. Now if the user chooses the parts of the image in an order so as to make the original image, he sent then the user is considered authentic. Else the user is not granted access. The system uses image segmentation based on coordinates. The coordinates of the segmented image allow the system to fragment the image and store it in different parts. Actually, the system segments the image into a grid and stores each part accordingly in order. But while logging in the image is shown as broken and in a jumbled order. At this time only the user who provided the image knows what the actual image looks like and he must the parts in the horizontal direction from left to right one row at a time according to the order in which parts were arranged in the original image. So, the user is granted access after a successful attempt.

PROBLEM STATEMENT

The drawback of this scheme is that the server needs to store a large number of pictures which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of portfolio images of each user in plaintext. Also, the process of selecting a set of pictures from a picture database can be tedious and time-consuming for the user. This scheme was not really secure because the passwords need to store in a database and that is easy to see. Sobrado and Birgit developed a graphical password technique that deals with the shoulder surfing problem. In their first scheme, the system displays a number of pass objects (preselected by the

user) among many other objects as shown. To be authenticated, a user needs to recognize pass objects and click inside the convex hull formed by all the pass objects. They developed many schemes to solve the shoulder surfing problem but the main drawback of these schemes is that the log-in process can be slow. Another recognition-based technique is proposed by Man et all He proposed a shoulder-surfing resistant algorithm which is similar to that developed by Sobrado and Birgit.

Our proposed system is an approach toward more reliable, secure, user-friendly, and robust authentication. We have also reduced the shoulder surfing problem to some extent.

1. The first step is to type the user's name and a textual password which is stored in the database. During authentication, the user has to give that specific user name and textual password in order to log in.
2. In this second step, objects are displayed to the user and he/she selects a minimum of three objects from the set and there is no limit for the maximum number of objects. This is done by using one of the recognition-based schemes.
3. During authentication, the user draws pre-selected objects as his password on a touch-sensitive screen (or according to the environment) with a mouse or a stylus. This will be done using pure recall-based methods.
4. In this step, the system performs pre-processing
5. In the fifth step, the system gets the input from the user and merges the strokes in the user-drawn sketch.
6. After stroke merging, the system constructs the hierarchy.
7. The seventh step is sketch simplification.
8. In the eighth step three types of features are extracted from the sketch drawn by the user.
9. The last step is called hierarchical matching.